UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,322	12/06/2001	Neil Andrew Cowie	550-290	4863

7590 09/06/2006

Zilka-Kotab, PC
P.O. Box
San Jose, CA 95172-1120

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/003,322	**Applicant(s)** COWIE ET AL.	
	Examiner Syed Zia	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 22 June 2006.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,9-16,21-28 and 33-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,9-16,21-28 and 33-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to request for reconsideration filed on June 22, 2006. Original application contained Claims 1-36.. Applicant currently amended Claims 1, 13, 25, and cancelled Claims 5-8, 17-20, and 29-32. The amendment filed on June 22, 2006have been entered and made of record. Presently Claims 1-4, 9-16, 21-28, and 33-39 are pending for consideration.

Response to Arguments

Applicant's arguments filed on June 22, 2006 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1-4, 9-16, 21-28, and 33-39 applicants argued that the system of cited prior art (CPA) [Abu-Husein (U. S. Patent 6,895,506), and further in view of Nachenberg (U. S. Patent 5,826,013)] does not teach, the subject matter as claimed.

Regarding Claims 1, 13, and 25 applicant argued that the system of cited prior art does not teach "loader program that triggers the execution of a computer program, malware scanning computer loader program, and replacing loader program with a clean copy".

Regarding dependent Claims, applicant also argued that in the system of cited prior art operable to terminate loader program, loading computer program into memory.

This is not found persuasive. The system of cited prior art clearly teach program storage and execution mechanism that has memory manager which deletes unencrypted version of program from memory after completion of program execution for securely storing and executing program on computer. A processor executes unencrypted version of a program written in a memory, to carry out a requested operation. A memory manager deletes the unencrypted version from memory, after completion of program execution. The memory manager also deletes decrypted program code, thus ensuring that decrypted code exists for only minimum necessary period. The computer virus detection module includes a CPU emulator for emulating a target program, and a virus signature scanning module for scanning decrypted virus code. An emulation control module includes a static exclusion module, a dynamic exclusion module, instruction/interrupt usage profiles for the mutation engines of the known polymorphic viruses, size and target file types for the viruses, and a table having an entry for each known polymorphic virus. During emulation, the emulation control module may observe use of a register-indirect memory write instruction using a register that has not been initialized (Abu-Husein: col.2 line 50 to col.3 line 4, and col.6 line 53 to col.9 line 15, and Nachenberg: col.9 line 50 to line 67 and col. 5 line 27 to line 39, and col.3 line 25 to line 53).

As a result, cited prior art does implement and teach a system and method that relates to scanning computer code for viruses and for providing results pertaining to the viruses found by scanning of the initiation of execution of a computer program using a mechanism that seeks to protect the computer program from malicious alteration.

Applicants still have failed to identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that cited prior art(s) does teach or suggest the subject matter recited in independent and dependent claims. Accordingly, rejections for claims 1-4, 9-16, 21-28, and 33-39 are respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-4, 9-16, 21-28, and 33-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Abu-Husein (U. S. Patent 6,895,506), and further in view of Nachenberg (U. S. Patent 5,826,013).

Regarding Claim 1 Abu-Husein teaches and describes a computer program product for controlling a computer to execute a computer program within a computer memory, said computer program product comprising: a loader program; and an encrypted version of said computer program; wherein said loader program is operable to: read said encrypted version of said computer program stored in a program store; decrypt said encrypted version of said computer program to form said computer program in an executable form; load said computer program directly into said computer memory; and trigger execution of said computer program as loaded into said computer memory by said loader program (col.2 line 50 to col.3 line 4, and col.6 line 53 to col.8 line 10).

Although the system and method disclosed by Abu-Husein shows all the features of the claimed limitation, such as loader, encrypting and decrypting the computer program (col.6 line 38 to line 45) but Abu-Husein does not specifically disclose malware, such as anti-virus computer program.

In an analogous art, Nachenberg, on the other hand discloses computing environment for detecting, such as scanning, polymorphic viruses, such as malware, and other malicious software (Nachenberg: Abstract), wherein:

said computer program that is decrypted, loaded, and executed includes a malware scanning computer program (col.3 line 3 to line 24).

said malware scanning computer program is operable such that once executed, said malware scanning computer program scans said loader program for malware (col.3 line 25 to line 53).

if said loader program is detected as being infected with said malware, then said malware scanning computer program is operable to repair said loader program or replace said loader program with a clean copy of said loader program (col.9 line 50 to line 67).

said malware scanning computer program is operable to scan for said malware including one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image (col.6 line 54 to col.7 line 8).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Abu-Husein and Nachenberg, because Nachenberg's method of detecting polymorphic viruses, such as malware, by using scanning engine, and a table having an entry for each known polymorphic virus would not only provide an extensible mechanism for malware definition data that can include program code operable to utilize the malware definition data for checking the signature of the malware scanner engine, but will also provide uniform mechanism of updating, and enforcing software authentication and protection (Abu-Husein: col. 10 line 28 to line 43).

Regarding Claim 13 Abu-Husein teaches and describes a method of executing of a computer program within a computer memory, said method comprising the steps of: executing a loader program, said loader program operating to: read an encrypted version of said computer program stored in a program store; decrypt said encrypted version of said computer program to form said computer program in an executable form; load said computer program directly into said computer memory; and trigger execution of said computer program; and executing said computer program as loaded into said computer memory by said loader program (col.2 line 50 to col.3 line 4, and col.6 line 53 to col.8 line 10).

Although the system and method disclosed by Abu-Husein shows all the features of the claimed limitation, such as loader, encrypting and decrypting the computer program (col.6 line

38 to line 45) but Abu-Husein does not specifically disclose malware, such as anti-virus computer program.

In an analogous art, Nachenberg, on the other hand discloses computing environment for detecting, such as scanning, polymorphic viruses, such as malware, and other malicious software (Nachenberg: Abstract), wherein:

said computer program that is decrypted, loaded, and executed includes a malware scanning computer program (col.3 line 3 to line 24).

said malware scanning computer program is operable such that once executed, said malware scanning computer program scans said loader program for malware (col.3 line 25 to line 53).

if said loader program is detected as being infected with said malware, then said malware scanning computer program is operable to repair said loader program or replace said loader program with a clean copy of said loader program (col.9 line 50 to line 67).

said malware scanning computer program is operable to scan for said malware including one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image (col.6 line 54 to col.7 line 8).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Abu-Husein and Nachenberg, because Nachenberg's method of detecting polymorphic viruses, such as malware, by using scanning engine, and a table having an entry for each known polymorphic virus would not only provide an extensible mechanism for malware definition data that can include program code operable to utilize the malware definition data for checking the signature of the malware scanner engine, but will also provide uniform mechanism of updating, and enforcing software authentication and protection (Abu-Husein: col. 10 line 28 to line 43).

Regarding Claim 25 Abu-Husein teaches and describes a apparatus for executing a computer program within a computer memory, said apparatus comprising: loader program logic; and a program store operable to store an encrypted version of said computer program; wherein said loader program logic is operable to: read said encrypted version of said computer program stored in said program store; decrypt said encrypted version of said computer program to form said computer program in an executable form; load said computer program directly into said computer memory; and trigger execution of said computer program as loaded into said computer memory by said loader program (col.2 line 50 to col.3 line 4, and col.6 line 53 to col.8 line 10).

Although the system and method disclosed by Abu-Husein shows all the features of the claimed limitation, such as loader, encrypting and decrypting the computer program (col.6 line 38 to line 45) but Abu-Husein does not specifically disclose malware, such as anti-virus computer program.

In an analogous art, Nachenberg, on the other hand discloses computing environment for detecting, such as scanning, polymorphic viruses, such as malware, and other malicious software (Nachenberg: Abstract), wherein:

said computer program that is decrypted, loaded, and executed includes a malware scanning computer program (col.3 line 3 to line 24).

said malware scanning computer program is operable such that once executed, said malware scanning computer program scans said loader program for malware (col.3 line 25 to line 53).

if said loader program is detected as being infected with said malware, then said malware scanning computer program is operable to repair said loader program or replace said loader program with a clean copy of said loader program (col.9 line 50 to line 67).

said malware scanning computer program is operable to scan for said malware including one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image (col.6 line 54 to col.7 line 8).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Abu-Husein and Nachenberg, because Nachenberg's method of detecting polymorphic viruses, such as malware, by using scanning engine, and a table having an entry for each known polymorphic virus would not only provide an extensible mechanism for malware definition data that can include program code operable to utilize the malware definition data for checking the signature of the malware scanner engine, but will also provide uniform mechanism of updating, and enforcing software authentication and protection (Abu-Husein: col. 10 line 28 to line 43).

2. Claims 2-4, 9-12, 14-16, 21-24, 26-28, and 33-36 are rejected applied as above rejecting Claims 1, 13, and 24. Furthermore, the system Abu-Husein and Nachenberg teaches and describes a computer program product for controlling a computer to execute a computer program within a computer memory, wherein:

As per Claim 2, said encrypted version of said computer program is encrypted with a private encryption key and said loader program is operable to decrypt said encrypted version of said computer program with a corresponding public key (Abu-Husein: col.3 line 24 to line 34, and col.5 line 48 to col.6 line 5).

As per Claim 3, said encrypted version of said computer program and said loader program are stored as separate computer files within a computer file store (Abu-Husein: col.3 line 34 to line 44,and col.6 line 6 to line 22).

As per Claim 4, said loader program is associated with initialization data specifying one or more of: a storage location of said encrypted version of said computer program; a key to be used in decrypting said encrypted version of said computer program; and parameters specifying how said computer program should be loaded into said computer memory for execution (Abu-Husein: col.6 line 53 to col.7 line 8).

As per Claim 9, said loader program is operable to terminate after triggering execution of said computer program (Abu-Husein: col.8 line 65 to col.9 line 15).

As per Claim 10, said computer program is operable to terminate said loader program when said computer program is triggered to execute by said loader program (Abu-Husein: col.8 line 65 to col.9 line 15).

As per Claim 11, said loader program is operable to load said computer program into a memory space within said computer memory separate from a memory space used by said loader program (Abu-Husein: col.9 line 16 to line 50).

As per Claim 12, said loader program is operable to load said computer program into an execution stream separate from an execution stream used by said loader program (Abu-Husein: col.9 line 16 to line 50).

As per Claim 14, said encrypted version of said computer program is encrypted with a private encryption key and said loader program decrypts said encrypted version of said computer program with a corresponding public key (Abu-Husein: col.3 line 24 to line 34, and col.5 line 48 to col.6 line 5).

As per Claim 15, said encrypted version of said computer program and said loader program are stored as separate computer files within a computer file store (Abu-Husein: col.3 line 34 to line 44,and col.6 line 6 to line 22).

As per Claim 16, said loader program is associated with initialization data specifying one or more of: a storage location of said encrypted version of said computer program; a key to be used in decrypting said encrypted version of said computer program; and parameters specifying how said computer program should be loaded into said computer memory for execution (Abu-Husein: col.6 line 53 to col.7 line 8).

As per Claim 21, said loader program terminates after triggering execution of said computer programs (Abu-Husein: col.8 line 65 to col.9 line 15).

As per Claim 22, said computer program terminates said loader program when said computer program is triggered to execute by said loader program (Abu-Husein: col.8 line 65 to col.9 line 15).

As per Claim 23, said loader program loads said computer program into a memory space within said computer memory separate from a memory space used by said loader program (Abu-Husein: col.9 line 16 to line 50).

As per Claim 24, said loader program loads said computer program into an execution stream separate from an execution stream used by said loader program (Abu-Husein: col.9 line 16 to line 50).

As per Claim 26, said encrypted version of said computer program is encrypted with a private encryption key and said loader program logic is operable to decrypt said encrypted version of said computer program with a corresponding public key (Abu-Husein: col.3 line 24 to line 34, and col.5 line 48 to col.6 line 5).

As per Claim 27, said encrypted version of said computer program and said loader program are stored as separate computer files within a computer file store (Abu-Husein: col.3 line 34 to line 44,and col.6 line 6 to line 22).

As per Claim 28, said loader program logic is associated with initialization data specifying one or more of: a storage location of said encrypted version of said computer program; a key to be used in decrypting said encrypted version of said computer program; and parameters specifying how said computer program should be loaded into said computer memory for execution (Abu-Husein: col.6 line 53 to col.7 line 8).

As per Claim 33, said loader program logic is operable to terminate after triggering execution of said computer programs (Abu-Husein: col.8 line 65 to col.9 line 15).

As per Claim 34, said computer program logic is operable to terminate said loader program when said computer program is triggered to execute by said loader program (Abu-Husein: col.8 line 65 to col.9 line 15).

As per Claim 35, said loader program logic is operable to load said computer program into a memory space within said computer memory separate from a memory space used by said loader program logic (Abu-Husein: col.9 line 16 to line 50).

As per Claim 36, said loader program logic is operable to load said computer program into an execution stream separate from an execution stream used by said loader program logic (Abu-Husein: col.9 line 16 to line 50).

As per Claim 37, wherein, as a first task, said malware scanning computer program scans said loader program for said malware (Nachenberg: col.3 line 25 to line 53).

As per Claim 38, if said loader program is detected as being infected with said malware, then said malware scanning computer program is operable to replace said loader program with a clean copy of said loader program (Nachenberg: col.9 line 50 to line 67 and col. 5 line 27 to line 39).

As per Claim 39, if said loader program is detected as being infected with said malware, then said malware scanning computer program is operable to repair said loader (Nachenberg: col.9 line 50 to line 67 and col. 5 line 27 to line 39).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
August 23, 2006